Discrete Mathematics 112 (1993) 93–102
North-Holland

On non-Abelian group difference sets*

Shuhong Gao

University of Waterloo, Department of Combinatorics and Optimization, Waterloo, Ont., Canada N2L 3G1

Wandi Wei

Sichuan University, Department of Mathematics, Chengdu, China

Received 12 February 1990

Abstract

Gao, S. and W. Wei, On non-Abelian group difference sets, Discrete Mathematics 112 (1993) 93–102.

This paper is motivated by Bruck's paper (1955), in which he proved that the existence of cyclic projective plane of order $n \equiv 1 \pmod 3$ implies that of a nonplanar difference set of the same order by proving that such a cyclic projective plane admits a regular non-Abelian automorphism group using n as a multiplier. In this paper we will discuss in detail the possibility of using multipliers to construct more non-Abelian difference sets from known difference sets, especially from cyclic ones. The existence of several infinite families of non-Abelian group different sets will be established.

1. Introduction

Let (G) be a group of order v. A k-subset D of G is called a (v, k, λ) difference set if the list of differences $d_1 d_2^{-1}, d_1, d_2 \in D$, contains each non-identity element of G exactly λ times. The number $n = k - \lambda$ is called the order of the difference set. A difference set D in G will be called non-Abelian, Abelian or cyclic provided G is non-Abelian, Abelian or cyclic, respectively. An automorphism α of G is called a multiplier of D if $D^\alpha = aDb$ for some a, b in G. When $D^\alpha = Db$ for some b in G, α is called a right multiplier. If G is Abelian, the mapping $\alpha_t : x \mapsto x^t$ (or $x \mapsto tx$ if G is written additively) is an automorphism of G for every integer t with $\gcd(t, v) = 1$. If α_t happens to be a multiplier, then it will be called numerical multiplier. In this case t is usually called a multiplier, though technically we should say α_t is a multiplier.

Correspondence to: Shuhong Gao, University of Waterloo, Department of Combinatorics and Optimization, Waterloo, Ont., Canada N2L 3G1.

*This research was supported in part by N.R.C. grant A3701.

Group difference sets are closely related to a type of incidence structure called symmetric block design. By a (v, k, λ) symmetric block design $\Pi=(V, \Theta)$ we mean a set V of v points and a collection Θ of v k-subsets (called blocks) of V such that each pair of distinct points is contained in exactly λ blocks. The number $n=k-\lambda$ is called the order of the design and when $\lambda=1$, a (v, k, λ) symmetric block design is also called a projective plane. An automorphism of a symmetric block design Π is a permutation on V which sends blocks to blocks. The set of all automorphisms of Π, denoted by Auto(II), forms a permutation group on V. Any subgroup of Auto(II) is called an automorphism group of Π. An automorphism group G of Π is said to be regular if for any two points x, y of Π there is a unique α in G such that $x^\alpha=y$. The following theorem describes an equivalence between difference sets and symmetric block designs.

Theorem 1. *Let $\Pi=(V, \Theta)$ be a (v, k, λ) symmetric block design admitting a group G of order v as a regular automorphism group. Let $x \in V$ and $B \in \Theta$ be arbitrarily chosen point (base point) and block (base block). Then*

$$D(x, B)=\{\alpha \in G \mid x^\alpha \in B\}$$

is a (v, k, λ) difference set. Conversely, if D is a (v, k, λ) difference set in G, then the incidence structure $\mathrm{dev}(D)=(G, \{D \cdot x \mid x \in G\})$ *with G as point set and $D \cdot x$, $x \in G$, as blocks is a (v, k, λ) symmetric block design with the right translation group $G_R=\{\tau_a \mid a \in G\}$ as a regular automorphism group, where $\tau_a: y \mapsto ya$, $y \in G$. And a right multiplier of a difference set is an automorphism of the corresponding block design.*

Remark. Though G_R is isomorphic to G, we will distinguish them in this paper. For any subgroup Δ of G, $\Delta_R=\{\tau_a \mid a \in \Delta\}$ is also a subgroup of G_R and any subgroup of G_R is of this form.

By this theorem we observe that from any difference set D in a group G we can develop a symmetric block design $\mathrm{dev}(D)$ with the right translation group G_R as a regular automorphism group. If the induced design $\mathrm{dev}(D)$ has other regular automorphism groups, then we obtain difference sets in these groups immediately. This is often possible as indicated by the following result due to Bruck [3].

Theorem 2. *If there is a cyclic planar difference set of order $n \equiv 1 \pmod 3$, then there is also a non-Abelian planar difference set of the same order.*

The proof of the theorem is simple, but it enables us to construct an infinite family of non-Abelian difference sets, since Singer [7] has proved that whenever n is a prime power there exists a cyclic planar difference set of order n. This stimulates us to carry on further. The most important point in Bruck's proof of Theorem 2 is using the multiplier n to construct a regular automorphism group of the induced plane. In this paper we apply this idea to a more general family of difference sets.

2. General observations

In an attempt to generalize Theorem 2 we naturally think of employing other numerical multipliers, even nonnumerical ones, other than the order n itself. We shall deal with the general case in this section.

Theorem 3. *Let D be a (v, k, λ) difference set in a group G of order v, θ a right multiplier of D with order r, $a \in G$ a fixed element. Let Δ be a subgroup of G and $\alpha = \theta\tau_a$, i.e.*

$$\alpha : x \mapsto x^\alpha = x^\theta a, \quad x \in G.$$

Then

$$\Gamma = \langle\alpha\rangle \cdot \Delta_R = \{\alpha^i \tau_b \mid b \in \Delta, i = 0, 1, 2, \ldots\}$$

forms a subgroup of Auto(dev$D$) *and acts regularly on the point set G of* dev(D) *if and only if the following conditions* (a) *and* (b) *are satisfied respectively:*

(a) *for each $b \in \Delta$, there is an integer j such that*

$$(1^{\alpha^{rj+1}})^{-1} b^\theta a = (a^{\theta^{r-1}} \cdots a^\theta a)^{-j} a^{-1} b^\theta a \in \Delta,$$

(b) *there is a factor w of m, which is the order of 1^{α^r}, such that*

$$\{1, 1^\alpha, 1^{\alpha^2}, \ldots, 1^{\alpha^{wr-1}}\} \tag{1}$$

constitutes a complete system of representatives of right cosets $x\Delta$, $x \in G$, of Δ in G.

Remark. After the first version of this work was finished, the authors were notified that Pott [6] also obtained this result in case $w = 1$ and α normalizes Δ_R (which implies that, in condition (a), $a^{-1} b^\theta a \in \Delta$ for each $b \in \Delta$).

Proof. Obviously $\Gamma \subset$ Auto(dev$D$). Observe that Γ forms a group if and only if for each $b \in \Delta$

$$\tau_b \alpha = \alpha^u \tau_{b_1} \tag{2}$$

for some integer u and $b_1 \in \Delta$. Let $u = rj + i$, $0 \leqslant i < r$. Noting that θ is an automorphism of G, we have

$$x^{\alpha^u} = x^{\theta^u} a^{\theta^{u-1}} \cdots a^\theta a = x^{\theta^i} 1^{\alpha^u}$$

for each $x \in G$. Equation (2) is equivalent to

$$x^\theta b^\theta a = x^{\theta^i} 1^{\alpha^u} b_1 \tag{3}$$

for each $x \in G$. Replacing x by the identity of G, we obtain $b^\theta a = 1^{\alpha^u} b_1$. Hence $x^\theta = x^{\theta^i}$ for each $x \in G$. So $i = 1$ and $(1^{\alpha^u})^{-1} b^\theta a \in \Delta$. But

$$1^{\alpha^u} = a^{\alpha^{rj}} = a^{\theta^{rj}} a^{\theta^{rj-1}} \cdots a^\theta a = a(a^{\theta^{r-1}} \cdots a^\theta a)^j,$$

so Γ forms a group if and only if condition (a) is satisfied.

Now we prove that when Γ is a group it acts regularly on G if and only if condition (b) is satisfied. Suppose that (b) is satisfied. Since (1) is a complete system of representatives of right cosets of Δ in G, we have $wr|\langle\Delta\rangle|=v$ and for any element x of G there must be an integer i and $b\in\Delta$ such that $x=1^{\alpha^i}b$. Then $1^{\alpha^i\tau_b}=x$, which proves the transitivity of the group Γ on G. To prove its regularity, we only need to prove $|\Gamma|=v$. Note that $\alpha^u\in\Delta_R$, say $\alpha^u=\tau_b$, $b\in\Delta$, if and only if

$$x^{\theta^u}a^{\theta^{u-1}}\cdots a^{\theta}a=x^{\theta^u}1^{\alpha^u}=xb \tag{4}$$

for each $x\in G$. Setting $x=1$ in (4) we have

$$1^{\alpha^u}=a^{\theta^{u-1}}\cdots a^{\theta}a=b \tag{5}$$

and thus

$$x^{\theta^u}=x \tag{6}$$

for each $x\in G$. Hence $\theta^u=1$ and $r|u$. Let $u=rj$. Then (5) means that

$$1^{\alpha^u}=1^{\alpha^{rj}}=(a^{\theta^{r-1}}\cdots a^{\theta}a)^j\in\Delta. \tag{7}$$

Since (1) represents all the right cosets of Δ in G, we have $1^{\alpha^{ri}}=(a^{\theta^{r-1}}\cdots a^{\theta}a)^i\notin\Delta$, for $1\leqslant i\leqslant w-1$, and $1^{\alpha^{rw}}=(a^{\theta^{r-1}}\cdots a^{\theta}a)^w\in\Delta$, thus w is the smallest positive integer i such that $1^{\alpha^{ri}}=(a^{\theta^{r-1}}\cdots a^{\theta}a)^i\in\Delta$. It follows from (7) that $w|j$. Hence $\alpha^u\in\Delta_R$ if and only if $(rw)|u$. Setting $b=1$ in the above discussion, we see that the order of α is rm, where m is the order of $1^{\alpha^r}=a^{\theta^{r-1}}\cdots a^{\theta}a$. So $|\langle\alpha\rangle\cap\Delta_R|=rm/rw$ and

$$|\Gamma|=\frac{|\langle\alpha\rangle||\Delta_R|}{|\langle\alpha\rangle\cap\Delta_R|}=wr|\Delta_R|=v.$$

Now assume that the group Γ acts on G regularly. Let d be the smallest positive integer such that $\alpha^d\in\Delta_R$. Then

$$1,\alpha,\ldots,\alpha^{d-1}$$

form a complete system of representatives of right cosets of Δ_R in Γ and thus

$$1,1^{\alpha},\ldots,1^{\alpha^{d-1}}$$

are representatives of right cosets of Δ in G. And furthermore, from above discussion, we see that $d=rw$ where w is the smallest positive integer such that $(a^{\theta^{r-1}}\cdots a^{\theta}a)^w\in\Delta$. Since $(a^{\theta^{r-1}}\cdots a^{\theta}a)^m=1\in\Delta$, we must have $w|m$. This completes the proof. □

Example 1. Let G be the elementary Abelian group of order 16 generated by a,b,c,d. It is easy to see that $D=\{1,a,b,c,d,abcd\}$ is a (16, 6, 2) difference set and θ, defined by

$$a^{\theta}=c,\qquad c^{\theta}=b,\qquad b^{\theta}=abcd,\qquad d^{\theta}=d$$

is an automorphism of G and fixes D. Let $\alpha=\theta\,\tau_a$ and $\Delta=\{1, ab\}$. It is routine to check that θ is of order 4, α is of order 8 and each of the two point orbits of G under $\langle\alpha\rangle$:

$$1\mapsto a\mapsto ac\mapsto abc\mapsto d\mapsto ad\mapsto acd\mapsto abcd\mapsto 1,$$

$$b\mapsto bcd\mapsto c\mapsto ab\mapsto bd\mapsto bc\mapsto cd\mapsto abd\mapsto b$$

is a complete system of representatives of cosets of Δ in G. Further, note that for each $x\in G$

$$x^{\tau_{ab}\alpha}=x^{\theta}(ab)^{\theta}a=x^{\theta}bd=x^{\alpha^5\tau_{ab}},$$

that is, $\tau_{ab}\alpha=\alpha^5\tau_{ab}$. Hence $\Gamma=\langle\alpha\rangle\cdot\Delta_R$ is a regular automorphism group of $\mathrm{dev}(D)$ by Theorem 3. By Theorem 1 we obtain a $(16, 6, 2)$ *difference set*:

$$\{1, \alpha, \alpha^4, \alpha^7, \alpha\beta, \alpha^3\beta\}$$

in $\Gamma=\langle\alpha, \beta\rangle$ with relations: $\alpha^8=\beta^2=1$, $\beta\alpha\beta=\alpha^5$, where $\beta=\tau_{ab}$.

Example 2. Let G and D be as in Example 1, θ be defined by:

$$a^{\theta}=b,\qquad b^{\theta}=a,\qquad c^{\theta}=d,\qquad d^{\theta}=c,$$

and $\alpha=\theta\tau_a$. Let $\Delta=\{1, c, d, cd\}$, $\beta_1=\tau_c$, $\beta_2=\tau_d$. Then it is easy to check that α and the subgroup Δ satisfy the conditions in Theorem 3 and $\Gamma=\langle\alpha, \beta_1, \beta_2\rangle$ with relations

$$\alpha^4=\beta_1^2=\beta_2^2=1,\qquad \beta_1\cdot\beta_2=\beta_2\cdot\beta_1,\qquad \alpha\cdot\beta_1=\beta_2\cdot\alpha$$

acts regularly on G. Hence we find that

$$\{1, \alpha, \alpha^3, \beta_1, \beta_2, \alpha^2\beta_1\beta_2\}$$

is a $(16, 6, 2)$ difference set in Γ.

The above two difference sets appeared in a different form in Kibler [5]. When Γ is cyclic, any multiplier is numerical. In this case Theorem 3 can be improved to the following simpler and more concrete form.

Theorem 4. *Let D be a (v, k, λ) difference set in the addition group of Z_v (the residue ring modulo v). If there is a multiplier t of D such that*

(a) *the order, say r, of t modulo v divides* $\gcd(v, 1+t+\cdots+t^{r-1})$, *and*

(b) *there is a factor w of m with the property that the smallest positive integer u with* $1+t+\cdots+t^{u-1}\equiv 0 \pmod{wr}$ *is equal to wr where* $m=v/\gcd(v, 1+t+\cdots+t^{r-1})$, *then there is a (v, k, λ) difference set in the group $\langle\alpha, \beta\rangle$ generated by α and β with orders mr and $v/(wr)$, respectively, which satisfy*

$$\alpha^{-1}\beta\alpha=\beta^t,\qquad \alpha^{wr}=\beta^s,$$

where $s\equiv(1+t+\cdots+t^{wr-1})/wr \pmod{v}$.

Proof. Apply Theorem 3. For any fixed $a \in Z_v$ with $\gcd(a, v)=1$, define α and β by

$$\alpha: x \mapsto tx + a,$$

$$\beta: x \mapsto x + wr.$$

Then $\alpha, \beta \in \mathrm{Auto}(\mathrm{dev}(D))$. Let Δ be the subgroup $\{wr\ x \mid x \in Z_v\}$ of Z_v. Then $\Delta_R = \langle \beta \rangle$ and $\Gamma = \langle \alpha, \Delta_R \rangle = \langle \alpha, \beta \rangle$. Note that

$$x^{\beta\alpha} = tx + twr + a = x^{\alpha\beta^t}$$

for each x in Z_v. So $\beta\alpha = \alpha\beta^t$ and $\Gamma = \langle \alpha \rangle \cdot \Delta_R$. So we only need to prove that the condition (b) in Theorem 3 is satisfied. Note that $m = v/\gcd(v,\ 1+t+\cdots+t^{r-1})$ is the order of $0^{\alpha^r} = 1+t+\cdots+t^{r-1}$ in the addition group Z_v. Since $r \mid \gcd(v,\ 1+t+\cdots+t^{r-1})$ and $w \mid m$, we have $wr \mid v$ and thus $|\Delta| = v/wr$. As rw is the smallest positive integer u such that

$$1+t+\cdots+t^{u-1} \equiv 0 \pmod{rw},$$

we see that $0, 1, 1+t, \ldots, 1+t+\cdots+t^{rw-2}$ are different modulo rw, that is, they form a complete system of representatives of cosets of Δ in Z_v. As $\gcd(a, v)=1$,

$$\{0, 1, 1+t, \ldots, 1+t+\cdots+t^{rw-2}\}$$

$$\equiv a\{0, 1, 1+t, \ldots, 1+t+\cdots+t^{rw-2}\} \pmod{rw}$$

$$\equiv \{0, 0^{\alpha}, 0^{\alpha^2}, \ldots, 0^{\alpha^{rw-1}}\} \pmod{rw}$$

represents the cosets of Δ in Z_v. This completes the proof. □

Example 3. We know that there is a cyclic difference set of parameters $(40, 13, 4)$ in Z_{40} and 3 and 9 are multipliers of it (refer to [1, 2]). For $t=3$, $r=4$ and $m=1$, Condition (b) in Theorem 4 is violated. But for $t=9$, we may get three non-Abelian $(40, 13, 4)$ difference sets (The first of which appeared in Kibler [5], the last two seem to be new).

(a) $t=9$, $r=2$, $m=4$, $w=4$:

$$D = \{\alpha, \alpha^4, \alpha\beta, \alpha^2\beta, \alpha^3\beta^2, \alpha^6\beta^2, \alpha\beta^3, \alpha^3\beta^3, \alpha^5\beta^3, \alpha^6\beta^3, \alpha^7\beta^3, \alpha^2\beta^4, \alpha^3\beta^4\}$$

in $\Gamma = \langle \alpha, \beta \rangle$ with the relations $\alpha^8 = \beta^5 = 1$, $\alpha^{-1}\beta\alpha = \beta^4$.

(b) $t=9$, $r=2$, $m=4$, $w=2$:

$$D = \{\alpha, \alpha^4, \alpha\beta^2, \alpha^2\beta^2, \alpha^3\beta^4, \alpha^6\beta^4, \alpha\beta^6, \alpha^3\beta^6, \alpha^5\beta^6, \alpha^6\beta^6, \alpha^7\beta^6, \alpha^2\beta^8, \alpha^3\beta^8\}$$

in $\Gamma = \langle \alpha, \beta \rangle$ with the relations $\alpha^8 = \beta^{10} = 1$, $\alpha^{-1}\beta\alpha = \beta^9$ and $\alpha^4 = \beta^5$.

(c) $t=9$, $r=2$, $m=4$, $w=1$:

$$D = \{\alpha, \alpha^4, \alpha\beta^4, \alpha^2\beta^4, \alpha^3\beta^8, \alpha^6\beta^8, \alpha\beta^{12}, \alpha^3\beta^{12}, \alpha^5\beta^{12}, \alpha^6\beta^{12}, \alpha^7\beta^{12}, \alpha^2\beta^{16}, \alpha^3\beta^{16}\}$$

in $\Gamma = \langle \alpha, \beta \rangle$ with the relations $\alpha^8 = \beta^{20} = 1$, $\alpha^{-1}\beta\alpha = \beta^9$ and $\alpha^2 = \beta^5$.

Example 4. We know that there is a cyclic difference set of parameters $(156, 31, 6)$ in Z_{156} and 5 and 25 are multipliers of it (refer to [1, 2]). Choosing $a=1$ in the definition of α, we may get, by Theorem 4, five new non-Abelian $(156, 31, 6)$ difference sets:

(a) $t=5$, $r=4$, $m=1$, $w=1$ (note that $1+5+5^2+5^3=156=v$):

$$D=\{1,\beta^7,\beta^{17},\beta^{19},\beta^{35},\alpha,\alpha\beta,\alpha\beta^3,\alpha\beta^6,\alpha\beta^{16},\alpha\beta^{29},\alpha\beta^{31},\alpha^2\beta^{10},$$
$$\alpha^2\beta^{13},\alpha^2\beta^{17},\alpha^2\beta^{20},\alpha^2\beta^{28},\alpha^2\beta^{29},\alpha^2\beta^{32},\alpha^2\beta^{34},\alpha^3\beta^2,\alpha^3\beta^6,$$
$$\alpha^3\beta^{14},\alpha^3\beta^{15},\alpha^3\beta^{20},\alpha^3\beta^{22},\alpha^3\beta^{23},\alpha^3\beta^{24},\alpha^3\beta^{28},\alpha^3\beta^{29},\alpha^2\beta\}$$

in $\Gamma=\langle\alpha,\beta\rangle$ with the relations $\alpha^4=\beta^{39}=1$, $\alpha^{-1}\beta\alpha=\beta^5$.

(b) $t=25$, $r=2$, $m=6$, $w=6$:

$$D=\{1,\alpha,\alpha\beta,\alpha\beta^2,\alpha^2\beta^4,\alpha^2\beta^5,\ \alpha^2\beta^8,\alpha^2\beta^9,\alpha^3\beta,\alpha^3\beta^5,\alpha^3\beta^7,\alpha^3\beta^8,$$
$$\alpha^3\beta^{10},\alpha^4\beta^2,\alpha^4\beta^{11},\alpha^5\beta,\alpha^5\beta^6,\alpha^5\beta^9,\alpha^7\beta,\alpha^7\beta^4,\alpha^7\beta^{11},\alpha^8\beta^3,$$
$$\alpha^8\beta^{10},\alpha^9\beta,\alpha^{10}\beta,\alpha^{10}\beta^6,\alpha^{10}\beta^7,\alpha^{10}\beta^{12},\alpha^{11}\beta,\alpha^{11}\beta^3,\alpha^{11}\beta^{12}\}$$

in $\Gamma=\langle\alpha,\beta\rangle$ with the relations $\alpha^{12}=\beta^{13}=1$, $\alpha^{-1}\beta\alpha=\beta^{12}$.

(c) $t=25$, $r=2$, $m=6$, $w=3$:

$$D=\{1,\alpha,\alpha\beta^2,\alpha\beta^4,\alpha^2\beta^8,\alpha^2\beta^{10},\alpha^2\beta^{16},\alpha^2\beta^{18},\alpha^3\beta^2,\alpha^3\beta^{10},\alpha^3\beta^{14},\alpha^3\beta^{16},$$
$$\alpha^3\beta^{20},\alpha^4\beta^4,\alpha^4\beta^{22},\alpha^5\beta^2,\alpha^5\beta^{12},\alpha^5\beta^{18},\alpha^7\beta^2,\alpha^7\beta^8,\alpha^7\beta^{22},\alpha^8\beta^6,$$
$$\alpha^8\beta^{20},\alpha^9\beta^2,\alpha^{10}\beta^2,\alpha^{10}\beta^{12},\alpha^{10}\beta^{14},\alpha^{10}\beta^{24},\alpha^{11}\beta^2,\alpha^{11}\beta^6,\alpha^{11}\beta^{24}\}$$

in $\Gamma=\langle\alpha,\beta\rangle$ with the relations $\alpha^{12}=\beta^{26}-1$, $\alpha^{-1}\beta\alpha=\beta^{25}$ and $\alpha^6=\beta^{13}$.

(d) $t=25$, $r=2$, $m=6$, $w=2$:

$$D=\{1,\alpha,\alpha\beta^3,\alpha\beta^6,\alpha^2\beta^{12},\alpha^2\beta^{15},\alpha^2\beta^{24},\alpha^2\beta^{27},\alpha^3\beta^3,\alpha^3\beta^{15},\alpha^3\beta^{21},\alpha^3\beta^{24},$$
$$\alpha^3\beta^{30},\alpha^4\beta^6,\alpha^4\beta^{33},\alpha^5\beta^3,\alpha^5\beta^{18},\alpha^5\beta^{27},\alpha^7\beta^3,\alpha^7\beta^{12},\alpha^7\beta^{33},\alpha^8\beta^9,$$
$$\alpha^8\beta^{30},\alpha^9\beta^3,\alpha^{10}\beta^3,\alpha^{10}\beta^{18},\alpha^{10}\beta^{21},\alpha^{10}\beta^{36},\alpha^{11}\beta^3,\alpha^{11}\beta^9,\alpha^{11}\beta^{36}\}$$

in $\Gamma=\langle\alpha,\beta\rangle$ with the relations $\alpha^{12}=\beta^{39}=1$, $\alpha^{-1}\beta\alpha=\beta^{25}$ and $\alpha^4=\beta^{13}$.

(e) $t=25$, $r=2$, $m=6$, $w=1$:

$$D=\{1,\alpha,\alpha\beta^6,\alpha\beta^{12},\alpha^2\beta^{24},\alpha^2\beta^{30},\alpha^2\beta^{48},\alpha^2\beta^{54},\alpha^3\beta^6,\alpha^3\beta^{30},\alpha^3\beta^{42},\alpha^3\beta^{48},$$
$$\alpha^3\beta^{60},\alpha^4\beta^{12},\alpha^4\beta^{66},\alpha^5\beta^6,\alpha^5\beta^{36},\alpha^5\beta^{54},\alpha^7\beta^6,\alpha^7\beta^{24},\alpha^7\beta^{66},\alpha^8\beta^{18},$$
$$\alpha^8\beta^{60},\alpha^9\beta^6,\alpha^{10}\beta^6,\alpha^{10}\beta^{36},\alpha^{10}\beta^{42},\alpha^{10}\beta^{72},\alpha^{11}\beta^6,\alpha^{11}\beta^{18},\alpha^{11}\beta^{72}\}$$

in $\Gamma=\langle\alpha,\beta\rangle$ with the relations $\alpha^{12}=\beta^{78}=1$, $\alpha^{-1}\beta\alpha=\beta^{25}$ and $\alpha^2=\beta^{13}$.

3. Special cases

Now we state a direct generalization of Bruck's theorem to a family of cyclic difference sets with parameters:

$$v=(q^{N+1}-1)/(q-1), \qquad k=(q^N-1)/(q-1), \quad \lambda=(q^{N-1}-1)/(q-1) \tag{8}$$

for $N\geqslant 2$ and q a prime power, their existence was established by Singer [7] in 1938.

Theorem 5. *Let q be a prime power and $N\geqslant 2$ an integer. If $q\equiv 1 \pmod{N+1}$, then there is a non-Abelian difference set with parameters* (8) *in the group $\Gamma=\langle\alpha,\beta\rangle$ generated by α and β with orders $N+1$ and $v/(N+1)$, respectively, which satisfy $\alpha^{-1}\beta\alpha=\beta^q$.*

Remark. This result is also obtained by Pott [6]. When $N=2$, this is Theorem 2.

Proof. Let D be a difference set in Z_v with parameters (8). We know by the multiplier theorems (refer to [2, 4]) that q is a multiplier of D. Setting, in Theorem 4, $t=q$ and v, k, λ as in (8), it is easy to see that the order of t modulo v is $N+1$. As $q\equiv 1 \pmod{N+1}$, we have

$$v\equiv 0 \pmod{N+1},$$

and

$$1+q+\cdots+q^N\equiv 0 \pmod{N+1}.$$

Note that $m=v/\gcd(v,\ 1+t+\cdots+t^N)=1$ and $N+1$ is the smallest positive integer u such that

$$1+q+\cdots+q^{u-1}\equiv 0 \pmod{N+1}.$$

The theorem follows immediately. □

Theorem 6. *Let q be an odd prime power and*

$$v=q^3+q^2+q+1, \qquad k=q^2+q+1, \qquad \lambda=q+1. \tag{9}$$

Then, for any positive integer $w|(q+1)$, there is a non-Abelian (v, k, λ) difference set in the group $\Gamma=\langle\alpha,\beta\rangle$ generated by α and β of orders $2(q+1)$ and $v/2w$, respectively, which satisfy

$$\alpha^{-1}\beta\alpha=\beta^{q^2} \quad \textit{and} \quad \alpha^{2w}=\beta^{(q^2+1)/2}.$$

Proof. Apply Theorem 4. We know that there is a cyclic difference set of parameter (9) and q^2 is a multiplier of it. Let $t=q^2$. Then the order r of t modulo v is 2. As q is odd, condition (a) is obviously satisfied. Observing that $v=(q+1)(q^2+1)$, we see that $m=v/\gcd(v,\ 1+t+\cdots+t^{r-1})=q+1$. Note that $q^2-1=((q-1)/2)2(q+1)$, we have $q^2\equiv 1 \pmod{2m}$ and thus $t=q^2\equiv 1 \pmod{2w}$. So

$$1+t+\cdots+t^{u-1}\equiv u \pmod{2w}.$$

This means that condition (b) is also satisfied. The application is completed by noting that $1+t+\cdots+t^{2w-1}\equiv w(1+t)\equiv w(1+q^2) \pmod v$. This proves the theorem. □

Example 4(a) is an example for Theorem 5. The remaining part of Example 4 and Example 3 are examples for Theorem 6. For the sake of Theorem 7, we first prove two lemmas.

Lemma 1. *Let p $(\neq 3)$ be an odd prime, q a prime, u a positive integer and $p|(q^{2u}+q^u+1)$. Let $t=q^{3u}$ and $v=q^{2pu}+q^{pu}+1$. Then $p\|(1+t+\cdots+t^{p-1})$, $p^c\|(t-1)$ and $p^{c+1}\|v$ for some integer $c\geqslant 1$.*

Proof. $p|(q^{2u}+q^u+1)$ implies that

$$t-1=q^{3u}-1\equiv 0 \pmod p. \tag{10}$$

Let $t=p^cw+1$, $p\dagger w$, $c\geqslant 1$. Note that

$$(q^{pu}-1)v=t^p-1=(p^cw+1)^p-1$$

$$\equiv \tfrac{1}{2}p(p-1)p^{2c}w^2+pp^cw+1-1 \pmod{p^{c+2}}\equiv p^{c+1}w \pmod{p^{c+2}},$$

we have $p^{c+1}\|(v(q^{pu}-1))$ and $p^{c+1}\|(t^p-1)$, hence

$$p\|(1+t+\cdots+t^{p-1}).$$

Now if $p|(q^{pu}-1)$, then

$$q^{2u}+q^u+1\equiv(q^{2u})^p+(q^u)^p+1\equiv 3 \pmod p,$$

contradicting the conditions that $p|(q^{2u}+q^u+1)$ and $p\neq 3$. Hence $p^{c+1}\|v$. This completes the proof. □

Lemma 2. *Let p,q,t,v be as in Lemma 1. Let $m=v/\gcd(v, 1+t+\cdots+t^{p-1})$. Then pm is the smallest positive integer w such that*

$$1+t+\cdots+t^{w-1}\equiv 0 \pmod{pm}. \tag{11}$$

Proof. Since the order of t modulo v is p, it follows that

$$(t-1)(t^{p-1}+\cdots+t+1)\equiv 0 \pmod v.$$

Hence $m|(t-1)$ and $1+t+\cdots+t^{w-1}\equiv w \pmod m$. Thus (11) implies that $m|w$. By Lemma 1 we see that $p|m$, so $(pm)|m^2$ and $(pm)|(mw)$. Let $t-1=mt_1$. Then

$$1+t+\cdots+t^{w-1}=(t^w-1)/(t-1)=((mt_1+1)^w-1)/(mt_1)$$

$$\equiv \tfrac{1}{2}w(w-1)mt_1+w \pmod{pm}\equiv w \pmod{pm}.$$

Therefore pm is the smallest positive integer w satisfying (11). This completes the proof. □

Theorem 7. *Let $p(\neq 3)$ be an odd prime, q a prime, u a positive integer, and $p|(q^{2u}+q^u+1)$. Let $v=q^{2pu}+q^{pu}+1$ and $m=v/\gcd(v, 1+q^{3u}+\cdots+(q^{3u})^{p-1})$. Then there is a non-Abelian planar difference set of order $n=q^{pu}$ in the group $\Gamma=\langle\alpha,\beta\rangle$ generated by α and β with order pm and $v/(pm)$, respectively, which satisfy $\alpha^{-1}\beta\alpha=\beta^{q^{3u}}$.*

Proof. We know that there exists a cyclic difference set with parameters

$$v=q^{2pu}+q^{pu}+1, \qquad k=q^{pu}+1, \qquad \lambda=1,$$

and q is a multiplier as well as q^{3u}. Let $t=q^{3u}$. Then the order of t modulo v is p and, by Lemma 1 and 2, t satisfies the three conditions in Theorem 4 with $w=m$. Our theorem follows from it immediately. □

For $p=7$ and 13 in Theorem 7 we have the following.

Corollary 1. *Let q be a prime. There exists a non-Abelian planar difference set of order $n=q^{7u}$ if q and u satisfy one of the following:*

(i) $q\equiv 2$ *or* $4 \pmod 7$, $u\equiv 1$ *or* $2 \pmod 3$;

(ii) $q\equiv 3$ *or* $5 \pmod 7$, $u\equiv 2$ *or* $4 \pmod 6$.

Corollary 2. *Let q be a prime. There is a non-Abelian planar difference set of order $n=q^{13u}$ if q and u satisfy one of the following:*

(i) $q\equiv 2, 6, 7$ *or* $11 \pmod{13}$, $u\equiv 4$ *or* $8 \pmod{12}$;

(ii) $q\equiv 4$ *or* $10 \pmod{13}$, $u\equiv 2$ *or* $4 \pmod 6$;

(iii) $q\equiv 3$ *or* $9 \pmod{13}$, $u\equiv 1$ *or* $2 \pmod 3$.

Note added in proof. The extended abstract of this paper has appeared in J. Sichuan University Natural Science Edition, Special Issue, 26 (1989) 136–139.

Acknowledgment

The authors would like to thank Professor Ronald C. Mullin and Dr. Alexander Pott for helpful suggestions and comments.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Math., Vol. 182 (Springer, Berlin, 1972).

[2] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographsches Institut, Mannheim, 1985).

[3] R.H. Bruck, Difference sets in a finite group, Trans. Amer. Math. Soc. 18 (1955) 464–481.

[4] M. Hall Jr, Combinatorial Theory, 2nd ed. (Wiley-Interscience, New York, 1986).

[5] R.E. Kibler, A summary of non-cyclic difference sets, $k\leqslant 20$, J. Combin. Theory Ser. A 25 (1978) 62–67.

[6] A. Pott, A generalization of a construction of Lenz, Proc. R.C. Bose Memorial Conf. on Comb. Math. and its Applications, Calcutta 1988, Sankhyā A, to appear.

[7] J. Singer, A Theorem in finite projective geometry and some applications to number theory, Trans, Amer. Math. Soc. 43 (1938) 377–385,